Angard Staffing
Acceptable Use Policy

Angard Staffing employees and workers assigned to Royal Mail may be authorised to access specified Royal Mail IT systems, applications, equipment and information where this is required to undertake their assignment. Access is limited to the systems and information required for their role and must only be used for authorised business purposes. This policy explains the rules that apply when using Angard and Royal Mail information, systems, applications and equipment.

Included in this policy:

- Purpose and scope
- Acceptable use
- Prohibited activity
- Security and account protection
- Email, messaging and internet security
- Social media and public communications
- Software and display content
- Personal devices, BYOD and Angard or Royal Mail applications
- Information classification and handling
- Monitoring and copyright
- Reporting and non-compliance
- Exceptions to this policy
- Where to go for more information
- Review

Purpose and scope

This policy applies to Angard Staffing employees and workers who access Angard or Royal Mail information, applications, equipment, networks, services or IT systems, whether directly or while on assignment. It explains the standards required to protect Angard, Royal Mail, colleagues, customers and services. Access to an Angard or Royal Mail application or system does not, by itself, constitute authority to use it.

Angard and Royal Mail systems are provided for authorised business use, and personal use is not permitted.

Within this policy, Royal Mail Group Ltd' will be referred to as 'Royal Mail'.

This policy does not form part of an employment contract and may be amended when required.

Acceptable use

When using Angard or Royal Mail equipment and systems, you must:

- Use systems, internet access, email and social media responsibly and only for authorised business purposes.
- Use approved secure connections, including any Angard or Royal Mail VPN or remote-access method required for the relevant system.
- Protect equipment and information from loss, damage, misuse and unauthorised access.
- Only store, download, upload or share business-related files and media.
- Follow all applicable Angard and Royal Mail security, data protection and conduct requirements.
- Only access, use or share the minimum amount of information necessary to complete the authorised business activity.
- Follow Angard or Royal Mail instructions, as applicable, for connecting, updating, restarting, charging, docking and maintaining any equipment issued or authorised for work.
- When using authorised devices away from an Angard or Royal Mail workplace, take appropriate precautions to prevent Angard or Royal Mail information from being seen, overheard or accessed by unauthorised people.
- Complete any mandatory data privacy, information security or cyber security training required by Angard or Royal Mail for the assignment and follow all applicable instructions and guidance.

Prohibited activity

You must not:

- Install unauthorised software, applications or plug-ins, uninstall approved software, or alter company equipment, systems, applications or security settings.
- Access, create, store or share illegal, offensive, discriminatory, threatening, inappropriate, gambling, pornographic or spam content.
- Open or forward suspicious files, emails or links that may introduce malware or compromise security.
- Share confidential information without appropriate authority and security controls.
- Share user IDs, passwords or login details, or use another person's account.
- Use company or personal devices in a way that affects productivity or business operations.
- Store, share, upload, copy or paste Angard or Royal Mail information to non-approved systems or technologies, including personal email, personal cloud storage, social media, messaging services or public/non-approved Artificial Intelligence (AI) tools.
- Connect a USB drive or other removable storage device to Angard or Royal Mail equipment unless this has been specifically authorised by the organisation responsible for the equipment or system.
- Use an Angard or Royal Mail email address to register for personal accounts, websites or services unless this is specifically required and authorised for business purposes.
- Leave Angard or Royal Mail equipment unattended in a public place or expose it unnecessarily to loss, theft or damage.

Security and account protection

Unauthorised access to, interference with or misuse of IT systems, software, data or information is strictly prohibited and may be treated as gross misconduct. This includes unauthorised deletion or alteration of information and may result in disciplinary action, dismissal and/or prosecution under the Computer Misuse Act 1990.

- Keep passwords and login credentials confidential and secure.
- Lock or log out of systems whenever leaving your workstation.
- Do not attempt to bypass security controls or access information without authorisation.
- Immediately report suspected phishing, lost or stolen equipment, unusual system behaviour, suspected unauthorised access, data incidents, accidental disclosure, security compromise or misuse through the applicable Angard or Royal Mail reporting route. Where an incident affects both organisations, notify both without delay.

Email, messaging and internet security

Spam, phishing and malicious content can seriously threaten systems and information. If an email or message is unknown or suspicious:

- Do not open or save attachments, click links, reply, or provide personal, financial or login information.
- Report it immediately through the appropriate reporting channels.
- Delete inappropriate, offensive or unsolicited commercial messages where appropriate.

Use only approved Angard or Royal Mail email and messaging services for business, selecting the service authorised for the activity. Company emails and messages must be professional, lawful and concise. Do not auto-forward company email to personal or unauthorised accounts, and do not include personal contact details in out-of-office replies.

Emails may be retained, monitored or retrieved for legal, regulatory and business purposes. Treat all email as a formal business record and do not disclose confidential information, make unauthorised commitments or inadvertently create contractual obligations.

Social media and public communications

Angard expects employees and workers to maintain the same standards of conduct online as in the workplace. Posts must not damage the reputation or brands of Angard or Royal Mail. Do not speak on behalf of either organisation unless authorised. Refer media enquiries relating to Royal Mail to the Royal Mail Group Director of Communications and follow the Social Media Policy.

Software and display content

Do not download unauthorised files, screensavers, wallpapers or software. Display content must not be obscene, pornographic, discriminatory, offensive or otherwise inappropriate under the Equality and Fairness Policy.

Personal devices, BYOD and Angard or Royal Mail applications

Angard employees and workers must not use a personal device to access Angard or Royal Mail applications, systems, information or data unless they have been specifically authorised to do so by the organisation responsible for that application, system, information or data.

Where access is authorised, it must only be used when required for the individual's current Angard assignment and for authorised business purposes. Having technical access does not, by itself, constitute authority to use a system or application.

Access must not be used outside the requirements of the assignment or following the end of an assignment. If Royal Mail or Angard withdraws authority, the individual must cease access immediately and remove or disable the application where instructed.

Angard or Royal Mail information must not be copied, downloaded, photographed, screen-captured, transferred or stored on a personal device unless the organisation responsible for the information has specifically authorised this.

Personal devices used for authorised access must be kept secure, protected by appropriate access controls and updated as required. Login credentials must not be shared and no other person may use the device to access Angard or Royal Mail systems or information.

Loss or theft of a personal device used for Angard or Royal Mail access, suspected unauthorised access or any other security concern must be reported immediately through the reporting route applicable to the affected organisation. Where both organisations may be affected, notify both without delay.

Where authorised, Angard workers may voluntarily use the Delivery App on a compatible personal device for delivery activities, with a PDA available as an alternative. Workers must follow the relevant safety guidance and training, ensure their device and charging cable is safe and suitable for use, and report any App, device, signal, or battery issues to their manager.

Information classification and handling

Angard and Royal Mail expect employees and workers to protect information according to the classification and handling requirements set by the organisation responsible for it. When working with Royal Mail information, Angard employees and workers must follow Royal Mail's classifications. When working with Angard information, they must follow Angard's applicable classification, privacy, retention and secure-handling requirements. Each classification or handling category defines the requirements for the appropriate access, storage, distribution, retention and disposal of information.

Classification	Required handling
Public	Information which is intended for public use, or which would have minimal impact on Royal Mail if lost or stolen. Examples; brochures or leaflets, information published on royalmail.com
Internal	Information for internal use only and not intended for public release. Examples; group-wide communications, meetings, material on the internet. The default classification is Internal.
Confidential	Information that has been assessed to be of a sensitive nature and likely to cause damage to Royal Mail's reputation following unauthorised disclosure. Examples: HR and payroll records, customer data.
Strictly Confidential	Very sensitive information that could harm our brand or expose Royal Mail to significant disadvantage should it fall into the wrong hands. Most people do not handle Strictly Confidential information. Example: unpublished financial results.

For information classified Internal you must:

- Only share it with employees of Royal Mail or other Angard employees and third parties who are authorised to receive it;
- Be vigilant when sending information via email. Check beforehand that the recipient details are correct;
- Lock it away in a secure place and never leave it unattended;
- Only use approved Angard or Royal Mail email, instant messaging, collaboration and internal mail facilities, as applicable, to share information. Do not use consumer-grade or personal systems, such as personal Gmail or messaging accounts;
- Ensure information related to any person, whether a colleague or a customer, is used appropriately and with their explicit consent;
- Be sensitive to discussing it in public areas where you can be overheard.

For Confidential and Strictly Confidential information you must also:

- Be authorised to email, copy distribute or upload it;
- Only use removable storage where this has been specifically authorised by the organisation responsible for the information or system. Where authorised, encrypt Confidential and Strictly Confidential information when storing it on a computer, sending it by email or saving it to approved removable or external storage;
- Dispose of it in the appropriate manner, shred it or place it in a confidential waste bin

Information handling requirements

- Access, use, share, store and dispose of information securely and only where authorised.
- Check recipients before sending information and use approved systems and security controls.
- Do not access another person's computer, account, files or printed information without authority.
- If information is sent to you in error, notify the sender and do not use, forward or disclose it.
- Keep information secure and avoid discussing sensitive matters where you may be overheard.
- Encrypt Confidential and Strictly Confidential information where required and dispose of it through approved confidential waste or destruction processes.

Monitoring and copyright

Angard and Royal Mail systems and services may generate records when they are used. Each organisation may collect, monitor, retain, audit and analyse information relating to the use of systems and technology for authorised legal, security and business purposes, in accordance with applicable law and its privacy information. Relevant information may be shared between Angard and Royal Mail where appropriate and lawful. Users should not expect use of Angard or Royal Mail systems and technology to be private. Users must not breach copyright or incur unauthorised costs when copying, downloading or sharing material.

Reporting and non-compliance

Failure to comply with this policy may result in Angard or Royal Mail suspending, restricting or removing access to its systems, applications, information or equipment. It may also result in investigation and disciplinary action under the Angard Disciplinary Policy.

All Angard or Royal Mail equipment, devices, access cards and other technology supplied or authorised for work must be returned, removed or disabled in accordance with the relevant

organisation's instructions when requested, when access is no longer required or when the assignment or employment ends. Individuals must not retain or continue to use either organisation's equipment, systems or applications after their authority has ended.

Serious breaches may lead to dismissal of gross misconduct for employees or termination of contract for contractors and agents. Any breach of the law may also result in criminal prosecution or civil action.

Individuals have a responsibility to report to the Angard Helpline Number 0333 240 8502 and email hr@angardstaffing.co.uk any breaches of this policy or any unauthorised use they are aware of. This includes inappropriate postings about Angard and Royal Mail, their employees, customers, partners or suppliers on the Internet or intranet.

Exceptions to this policy

Any exception relating to the use of Angard or Royal Mail systems, technology or information must be formally authorised through the appropriate process of the organisation responsible for the relevant system, technology or information. Where both organisations are affected, approval may be required from both. Angard employees and workers must not assume that an exception applies without explicit authorisation.

Where to go for more information

For questions about this policy, contact the Angard Helpline on 0333 240 8502 or email hr@angardstaffing.co.uk. For web access go to: www.angardstaffing.co.uk

In the event of any inconsistency between this policy and the supporting guides, the terms of this policy take precedence.

Further guidance is available in the Angard Social Media Policy and Angard AI Policy.

Review

This policy may be reviewed to ensure it remains effective and updated from time to time to meet Angard's requirements.

Date of last review: 25th November 2026